BIOCATCH
Less Friction • Less Fraud

January 10, 2017

Robert deV. Frierson
Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue, NW
Washington, DC 20551

Legislative and Regulatory Activities Division
Office of the Comptroller of the Currency
400 7th Street, SW
Suite 3E-218, Mail Stop 9W-11
Washington, DC 20219

Robert E. Feldman
Executive Secretary
Federal Deposit Insurance Corporation
550 17th Street, NW
Washington, DC 20429

Dear Sirs:

Thank you for considering the below comments in connection with the proposed Enhanced Cyber Risk Management Standards.

BioCatch is a cybersecurity company that delivers behavioral biometrics, analyzing human-device interactions to protect users and data. BioCatch works with the retail, corporate and wealth management departments of major banks around the world, primarily out of Europe and Latin America, providing continuous authentication for more than 2 billion transactions per month. Each week, we save our customers millions of dollars in fraud-related losses, and more importantly, we provide their clients an assurance that their personal information and money are safe. The most interesting thing that we see, is that our customers already employ multi-factor authentication, PINs, tokens, passwords, challenge/responses, physical biometrics, device authentication, IP verification and other fraud prevention solutions, yet they are still susceptible to intrusions. Time and time again, we are recognizing fraud situations that these other methods are not detecting.

We support the approaches that are outlined in the Request for Comment and believe that all stakeholders – banks, consumers and regulators – have a role to play in securing our financial systems and protecting the integrity of our institutions. Our comments pertain to the sections that relate to our core areas of expertise, namely fraud prevention and authentication in the context of internal and external dependency management, as well as cyber resilience and situational awareness.

(17) The agencies request comment on the comprehensiveness and effectiveness of the proposed standards for internal and external dependency management in achieving the agencies' objective of increasing the resilience of covered entities, third party service providers to covered entities, and the financial sector.

BioCatch believes that it is important to address all aspects of the financial service ecosystem in order to increase system-wide resilience. As the draft points out early on, "due to the interconnectedness of the U.S. financial system, a cyber incident or failure at one interconnected entity may not only impact the safety and soundness of the entity, but also other financial entities with potentially systemic consequences." The same holds true for consequences associated with large-scale data breaches. Today's cybercriminals are mining for information that allows them to access systems directly, either via social engineering or by installing malware on a victim's machine that allows them to operate freely, or by stealing credentials and personal information to be able to access other systems (this is possible because most people use similar passwords or variations of the same password across all their devices and applications). When monies are lost or stolen, or hackers take over people's accounts, the integrity of the entire system is put in question. It is not enough to focus on internal factors only; including external dependency in the proposed standard ensures that resilience beyond the corporate infrastructure to protect the consumers and ultimately the corporation itself.

(19) How do the proposed internal and external dependency management standards compare with processes already in place at banking organizations?

We believe that in the absence of a strong regulatory framework, and the different rules that financial institutions have to comply with, it is inevitable that some will look to raise the bar and others will seek minimum compliance. Some banks are reporting that compliance is eating up to 40% of their IT budgets, which means there is little room for advancing or creating new and stronger processes for their organizations. It is incumbent on the Agencies and other regulatory bodies to provide meaningful and clear guidance that addresses today's cyberthreats and raises the bar on best practices.

(27) What other factors should be included within the incident response, cyberesilience, and situational awareness category?

It is important that risk factors pertaining to social engineering, account takeover and malware be included in the cyber resilience and situation awareness category. While most guidelines and policies focus on identity management and access for login, the primary threat today comes from criminals who are able to circumvent all the authentication elements, including PINS, passwords, tokens, SMS messages, challenge/response questions and even physical biometrics. With malware or social engineering tactics, users are fooled into turning over credentials, providing third parties access to their machines or allowing them to take over remote sessions. Recognizing these threats via continuous authentication post-login is an important element to increasing resilience and maintaining heightened situational awareness.

(28) What additional requirements should the agencies consider to improve the resilience or situational awareness of a covered entity or the ability of a covered entity to respond to a cyberattack?

The Agencies are strongly encouraged to consider requirements for continuous authentication post login to improve the resilience and situational awareness of a covered entity. Technologies that enable continuous authentication typically work passively in the background and do not interfere with a user's experience on a website or mobile application. Behavioral biometrics specifically, establish user profiles based on way people interact with a device or an application such as scrolling or typing patterns, the use of shortcuts and how a person toggles between fields and responds to "invisible challenges". Invisible

challenges are tests that are invoked in the system and elicit a response without the user being aware. The most advanced behavioral biometric systems are able to collect more than 500 parameters of behavior and assign a profile to each user that is based on the 20 parameters that are most unique to them; the end result being each person's profile is based on different parameters. What this means for the fraudster is that (a) he doesn't know how he is supposed to behave to trick the system, unlike a known password or code that can be stolen and (b) he doesn't know when the system is testing him. This makes it possible to detect in real-time whether there is a breach being conducted by another human, or a piece of malware or a robot that is directing activity on a person's account.

Thank you again for your consideration of the above comments. We would welcome the opportunity to provide further information at any time. Please feel free to reach me at +1 917 862 1373 or by email at frances.zelazny@biocatch.com.

Regards,

Frances Zelazny
Vice President